VIEW POINT

THE ESG EVOLUTION AND CONVERGENCE WITH GRC – A BROAD PERSPECTIVE

Abstract

In the recent times, Environment, Social, and Governance (ESG) has evolved much beyond the earlier boundaries of sustainability or Corporate Social Responsibility (CSR). Today it is also linked to how IT systems and processes are managed, especially from security and privacy perspective, and the related governance and risks around it, while meeting compliance requirements. Technological companies, regulators, analysts, and investors have started looking at this aspect as a hygiene factor for good corporate governance including enhanced transparency and disclosure expectations. Thus, ESG is emerging as an overlapping function with Governance Risk and Compliance (GRC). As some of the reference data, analytics and key objectives will remain common, this has necessitated organizations to converge and integrate activities around both these functions, to leverage synergies, efficiencies, and effectiveness.

Infosys®
Navigate your next

The ESG evolution:

Though the present-day concept (and the term) of ESG took shape in the mid 2000's, through interventions which were driven by the UN, various nations and regulators, the related fundamental principles are dated back to decades or even centuries, with key milestones in this journey focusing on improving labor conditions during the industrial revolution, funding of wars or oppressive regimes like apartheid.

The current form of ESG refers to *organizational behavior* around aspects such as climate change vulnerability, renewable energy, supply chain labor standards, community relations, diversity equity and inclusion, privacy, data security, among many others. It is aimed at enhancing sustainability and resilience of organizations, economies, and nations – which is critical in an interconnected ecosystem, where a broken link could potentially impact the whole chain.

ESG has often been mistaken as CSR or environment sustainability, with a marketing or branding focus. There has been an increased awareness around this, due to the additional focus from technology companies, regulators, analysts, and investors. The business impact of ESG is seen as much broader - around building customer loyalty, providing competitive advantage, improving financial performance, attracting investors, and ensuring sustainable operations. This has led to ESG becoming a key component in board discussions and standard corporate governance reporting and disclosures. Organizations are expected to demonstrate integrity, ensuring the practice of values, ethics, statements, commitments, relationships, and transactions.

The recent years have witnessed a shift in investors paying lot of attention to the ESG scores of companies to invest in (in turn on the *purpose of organizations,* beyond the financial goals). There has been an increased focus on sustainable companies who demonstrate a positive impact on the environment and commits to ethics and compliance. This in turn has led Boards and CXOs to focus on ESG which represents the broad social commitments, backed by visible measures to define, enforce, measure, report and improve over a period.

The IT and Security/Privacy dimensions of ESG

Due to rapid digitization in the recent decades, corporate commitments and actions around ESG are now closely linked to IT systems and processes, especially from security and privacy perspectives, and the governance and risks around it, while adhering to compliance requirements – in short, building and sustaining digital trust with all stakeholders. This is largely due to the fact that 2.5 quintillion bytes of data is produced every day, thus necessitating best practices to collect, use, store or dispose data in a controlled manner balancing between business requirements, innovation and legal, social, ethical, transparency, and disclosure expectations. Consumer data adds significant value to businesses, hence as a social value, data privacy and security gains prominence as an integral part of an ESG program. Some of the key aspects around this are as follows:

- Supply chain security controls: To ensure overall supplier ecosystem is managed in a controlled manner, with adequate checks and balances
- Robust data governance: To cover the entire data lifecycle, with additional focus on cloud / SaaS environments
- Data minimisation: Being ecologically responsible, minimise resource collection, and usage to reduce e-waste, scope 3 emissions and carbon footprint
- Data privacy: Organizations should understand the following
  - Purpose of data collection: Collect only what is necessary
  - Openness: Focus on transparency, choice, consent – prioritizing people over profits
  - Transparency and disclosures: On how data gets used or distributed/shared, including related to AI/ML/biometrics
  - Responsible AI: Ensuring data analytics approaches follow standard norms and applicable regulations
- Data breach notification: Have systems and processes as per applicable regulations, to disclose the breach within stipulated time to those affected, the public, or government agencies
- Other security aspects: Network security, remote access, insider threats, security awareness training etc.

The ESG scores by ratings agencies

An *ESG score* is a quantitative metric rating (a numerical score or letter), assigned to an organization, for its ESG efforts. It includes a variety of ESG metrics, which can be used by stakeholders including investors and analysts to assess the risk and opportunities associated with the organization's practices. These scores help organizations identify risks (or areas to improve) in their ESG practices and plan for upliftment, benchmark against competitors within the same domain, and attract investors etc.

There are multiple third-party providers offering ESG scoring services. MSCI is one of the most popular providers of ESG scores, with comprehenssive rating of approximately 8,500 corporations. They use a rule-based methodology that identifies the key issues, risks and opportunities faced by an organization within the context of its industry vertical. Others include Bloomberg, Fitch, S&P Global, Moody's, ISS, Refinitiv, RepRisk, and Sustainalytics.

The computation of ESG score is complex as multiple parameters are considered with different weightages. However, each provider uses their proprietary algorithm to compute the score, and not a consistent approach. An illustrative view from MSCI ESG scoring is as follows:

Overall Grade	Numerical score	Letter Score
Leader	5.714 to 10.000	AA to AAA
Average	2.857 to 5.713	BB, BBB, or A
Laggard	<=2.856	CCC or B

GRC and ESG – Leveraging synergies, focussing on security and privacy contexts

Cybersecurity and privacy are often included as key components in the ESG scores by rating agencies. e.g.- The ESG scores from MSCI ESG Research has 29% weightage for cybersecurity and privacy for retail companies, and 28% for telecom and 20% for healthcare sector.

When a data breach happens, apart from financial and reputational impact, it also affects the ESG score. However, maturity on the due diligence and due care measures play an important part here, especially on the systems and policies/ processes in preventing, detecting, responding, containing, reporting any incident. Having independent audits as well as third party assurance around ISO27001, ISO27701, SOC2 or PCI-DSS etc could be an added advantage.

In this scenario, we can consider leveraging GRC, which has been an integration of capabilities that can help organizations attain their objectives and goals, analyse uncertainties, and conduct actions with integrity and honesty. It means organizations must have structured governance, SMART metrics reporting and manage the risks ensuring compliance to regulations and standards.

These activities need be handled in a streamlined and standardized manner maximising visibility and value to stakeholders. This can be done through tools/platforms which leverage workflow automation and AI techniques for improved efficiency and predictability.

With GRC and ESG emerging as a powerful duo in guiding organizational behavior and decision-making, with significant overlaps in goals, organizations with robust GRC programs are better equipped to manage ESG risks and opportunities to improve ESG performance.

From a GRC front, organizations could leverage standards/ frameworks from ISO, COSO, ISACA, IIA, and NIST. Another approach would be the open source OCEG GRC capability model, with processes (Learn, Align, Perform, and Review) providing a detailed pathway for companies to competently report ESG targets.

While the agencies providing ESG ratings have their own approaches to assess the security and privacy of enterprises, the level of subjectivity or biases can be minimized. This can be done if authentic data is available around publicly attested security and privacy programs, policies, processes, reporting with named security/privacy leaders holding accountability etc. Hence as a matter of mature corporate governance practices, organizations also can follow an internal analysis and scoring process using a standardized framework such as the Global Reporting Initiative (GRI - the popular third-party framework widely used by companies to assess their ESG performance within common categories and produce ESG reports using standardized criteria) or other standards/frameworks from IFRS, SASB, CDSB, CDP etc. too.

Organizations can look at designing a contextualized and unified framework by leveraging the best of both (GRC and ESG) frameworks and standards to design and manage an integrated program, aided by cross-functional collaborative teams, investment in appropriate technology platform(s) and data management, stakeholder engagement and transparency, as well as continuous improvement and learning. This integrated approach helps to improve effectiveness and efficiency, with assurance of quality outcomes with a holistic perspective.

Conclusion

With ESG gaining wider focus and attention from all stakeholders and emerging from a narrow soft reporting requirement to a broad regulated commitment with multiple dimensions, organizations could leverage the best of their GRC programs and draw benefits from an integrated approach. This helps in achieving the converged goals in a more predictable, effective, efficient manner, especially when organizations face complex structures, business models, large datasets, diverse and emerging regulatory requirements.

Infosys Cybersecurity Practice, through its GRC and Consulting & Advisory service offerings, backed by our technology partners, provides advice and support to its customers in their journey towards meeting the enterprise goals from all these perspectives, through a holistic long term strategic approach across people, process, and technology aspects, towards maximized value.

References:

1. Why data security and privacy can become a key ESG opportunity - BusinessToday
2. The Role of Data Privacy and Security in ESG (Environmental, Social, Governance) (ardentprivacy.ai)
3. Building trust with ESG, cybersecurity and privacy: PwC
4. privacy-and-data-security-in-esg.pdf (huntonak.com)
5. oceg.illustration.esg_.2022.pdf (workiva.com)
6. GRC Capability Model (Red Book) FULL VERSION - OCEG
7. ES-G-RC – The Role of GRC in Delivering ESG | GRC 20/20 Research, LLC (grc2020.com)
8. How to leverage your GRC program for ESG | Wolters Kluwer
9. The Importance of GRC And Why It Matters In ESG? (esgenterprise.com)
10. Power What's Next in ESG: Integrate GRC and ESG (metricstream.com)
11. Sustainability governance, risk and compliance solution | EY Luxembourg
12. Understanding Data Security & Privacy in ESG (skillcast.com)
13. MOVEit, Capita, CitrixBleed and more: The biggest data breaches of 2023 | TechCrunch
14. The History of ESG & Timeline Infographic | Origins of ESG (thesustainableagency.com)
15. What is the history of ESG? - The Corporate Governance Institute
16. Case Study: integration of both ESG and GRC | LinkedIn
17. 8 Top ESG Reporting Frameworks Explained and Compared (techtarget.com)
18. https://www.techtarget.com/sustainability/definition/ESG-score

About the Author

Oommen Thomas,

Head of GRC Practice and Consulting & Advisory Delivery – Infosys Cybersecurity

Oommen Thomas manages key strategic initiatives for the CyberSecurity practice at Infosys, including leading the GRC Practice and Consulting Delivery – devising and executing strategies for industry leading offerings and optimal business aligned solutions for global customers. He is an enthusiast on innovations in the Cybersecurity, Governance Risk and Compliance, AI and Data Privacy domains, and has been actively associated with security/privacy/management communities including through forums like ISACA, IAPP and PMI. A continuous learner with over 3 decades of IT industry experience spanning multiple domains, geographies, roles, and functions. Oommen's industry certifications include CISSP, CGEIT, CRISC, CISM, CSX-P, CPISI, ISO27001-LA, DP/GDPR-LI, CIPP/E, CIPM, FIP, TOGAF, PMP and ITIL. He has volunteered for IAPP serving on their Global Diversity in Privacy Advisory Board, and as Co-Chair for the IAPP Pune Chapter.

For more information, contact askus@infosys.com

Infosys®
Navigate your next